Advance Key Management Approach for Security in WSN

Falguni Saxena[1], Ketan Patel[2]
[1]Grow More Faculty of Engineering Himatnagar, Gujarat, India
[2] Ass.Prof., Grow More Faculty of Engineering Himatnagar, Gujarat, India

Abstract- **Wireless Sensor Network has higher count of tiny sensor nodes in network. To perform the operations such as data transfer, communications, token transfer etc. at each node requires energy. For secure communication between Ch to Node and Ch to BS, Certificate-Less Effective Key Management (CLEKM) protocol is used. The Cluster Head (CH) which has cluster key for the purpose of forwards message's inside the cluster. Pair-wise key shares the key to every node present in neighbor. The collected information is forwarded securely to base station by making use of individual key. When asymmetric schemes are used, maintenance of keys is easier, but they provide a lesser degree of security when compared to symmetric encryption schemes. In order to cope up with these shortcomings, we propose to use an improved version of the hybrid encryption scheme, which is a combination of Advanced Encryption Standard (AES) and Elliptical Curve Cryptography (ECC) with cross encrypted keys for secure key exchange and node authentication and hybrid encryption for enhanced cipher-text security.**

Index Terms- **Energy, Delay, Node, Performance.**

I. INTRODUCTION

A. WSN:

Wireless Sensor Network (WSN) has a various number of sensor nodes, having batteries to power them, having sensing, and data processing as well as radio communication components of short-range. The uses of WSNs varies from the best known, such as monitoring environment as well as automation of house, to ones which requiring much skill or efforts such as military or areas of security such as battlefield observations. Still in the WSN, the close communication between sensor nodes as well as operation performed by them, and the non-presence of physical protection make WSNs defenseless to a large range of network level threads also it can be cause due to physical damage. Despite sensor nodes have in built tamper-resistance technique, the memory chips have different memory read-out exposure.

As we studied WSN is used for compunction with sensitive information Thus, the communications in these networks must be secure. Securing the communication in WSN is a very important issue, just because of many security threats and because of the nature of WSN. We can notice this point by studying the communication links in these networks, which is the radio links that is subject to many faulty information and malicious attacks. Sensor devices in general have a limitation in its resources; these limitations can control the nature for WSNs, also affect the security level for this type of networks. As an example for such limitations; limited processing power, battery age, transmission distance, shortage in memory space, random distribution for nodes, and bandwidth [2].

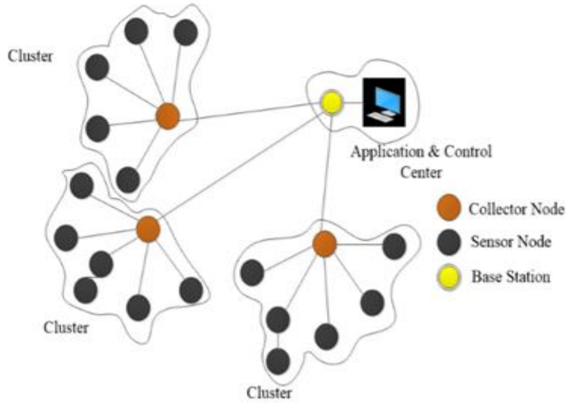


Fig.1 WSN Structure

B. Types of Keys

- Certificate less public /private key: The base station at the key generation Centre (KGC) creates a pair of certificate less public /private key and uses that key to the node before the node gets deployed.

- Individual node key: The different key was used for the each node with the base station. For example: L sensor sends the encrypted message with the individual key to the H sensor and alert message were sent to the base station or if it is fails to communicate

- Pairwise key generation: For a secure communication and node authentication a pairwise key were created between neighboring nodes. For example: L sensor and H sensor uses the same pairwise key. L sensor sends the encrypted message securely using pairwise key to the cluster. H sensor encrypts that required message to the cluster with the pairwise key.

- Cluster key: A key was shared to all the nodes in the cluster. The cluster key is used to secure the message which is sensitive. Cluster key was update by the cluster head during forward and backward secrecy.

C. Phases of CL-EKM

The CL_EKM includes the phases of system setup, pairwise key generation, cluster formation, key update, node movement and node revocation.

A.SYSTEM SETUP-Base station generates the parameters and node gets register before the deployment of network by including it in a member list.

-Generation of System Parameters

-Node Registration

B. PAIRWISE KEY GENERATION-To activate the pairwise key setup, a node transmit an advertised message to the neighborhood cluster nodes after the network has deployed. The advertised message includes its identifier and public key.

i) PAIRWISE MASTER KEY ESTABILISHMENT-The protocol was described for the establishment of pairwise master key between the two nodes nA and nB. An encapsulation process was used here between nA and nB for secure message transmission.

ii) PAIRWISE ENCRYPTION KEY ESTABILISHMENT-The HMAC of KAB was generated when the pairwise master key get generated. The node nA and nB was validated by HMAC. The pairwise encryption key established the HMAC value once the validation gets succeed.

C. CLUSTER FORMATION-After the node deployment H sensor creates L sensor in the course of signal message exchange and authenticated. If the process of authentication is succeeding, cluster were formed by H sensor with the help of L sensor which shares a same cluster key. Each member of cluster establishes a pairwise key

D. KEY UPDATE- Frequent key updating requires protecting against the attacker and cryptanalysis. In this process pairwise key update and cluster key update operations were done.

E. NODE MOVEMENT- In order to ensure forward and backward secrecy the cluster key should be properly managed by H sensor during the node movements. Thus the cluster key was update by the H sensor and base station gets notified about the changes of node status. By the use of this report the base station instantly revise the node status in the list.

F. KEY REVOCATION-To perceive malicious attacks the base station uses the intrusion detection system. By the use of node status information cluster head examine the abnormal node when the node leaves and node join the cluster the node status information gets update to the base station in the member list.

attackers are varied throughput is increased. With detection scheme provides better throughput compared to existing without detection scheme.

D.AES

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption. In December 2001, the National Institute of Standards (NIST) approved the AES as Federal Information Processing Standards Publication (FIPS PUB) 197, which specifies application of the Rijndael algorithm to all sensitive classified data. The Advanced Encryption Standard was originally known as Rijndael.

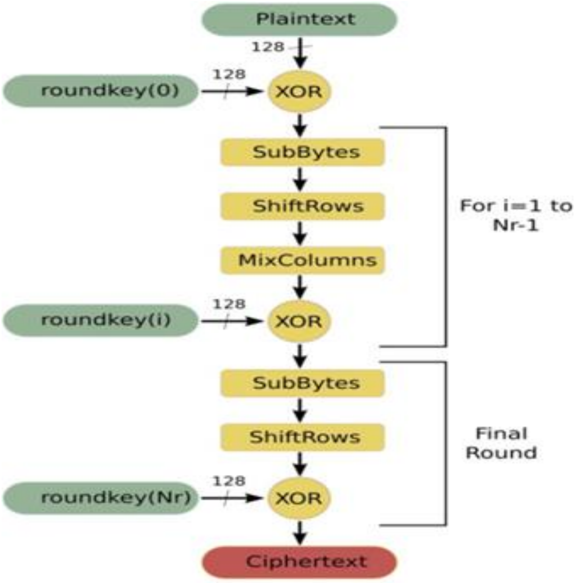


Fig.2 Flow of AES

E.ECC

Elliptical curve cryptography (ECC) is a public key encryption technique. It is based on the elliptic curve theory that can be used to create quicker, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation. This technology can be used in association with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some analysts, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC provide equivalent security with reduced computing power and battery resource usage, it is becoming widely used for mobile applications. Many companies, along with 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW, and VeriFone have included support for ECC in their products.

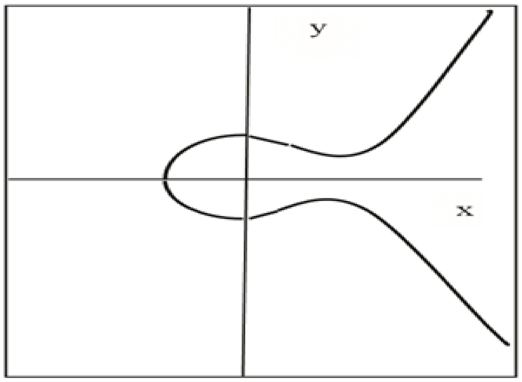


Fig.3 Sample elliptic curve

II.RELATED WORK

Paper, ECL-EKM: An Enhanced Certificateless Effective Key Management Protocol for Dynamic WSN researched over CL-EKM and their limitation in WSN. They founded that this protocol shows some critical limitations. One among these is the method of relying on unicast transmission mode to transmit messages from the Base Station (BS) to all cluster heads in the network. So that they consider the optimization problem of the protocol and propose a solution which enhances CL-EKM by avoiding intensive use of encryption and unicast operations that reduces the energy and delay associated with the communications between the BS and the cluster heads.

III.PROPOSED WORK

In existing system they are not using hybrid encryption scheme [1]. They are using EB Based Message Broadcasting system. Key generation is based on AES. We proposed a new Hybrid Solution for additional security to ECC keys. Elliptic Curve Cryptography is the most recommended PKC for low power, computationally constrained sensors [3]. Different applications of WSN require different levels of security varying from basic security to high level of security. To decide The three main factors that decide the choice of the parameter values of EC for constrained WSN security solution (ECC) are the level of security desired, the communication environment and constraints/capabilities of the application platform.

Flow and Steps for the CL-EKM are described as below.

Steps CL-EKM

Step 1: System Setup
BS, CH, Network size, Energy, KGC

Step 2: Pairwise Key Generation using AES+ECC

Step 3: Cluster Formation
Membership Assignment, CH Selection

Step 4: Key Updation
Key Updation of Pairwise Key and Cluster Key

Step 5: Node Movements
Cluster Join/Leave

Step 6: Key Revocation

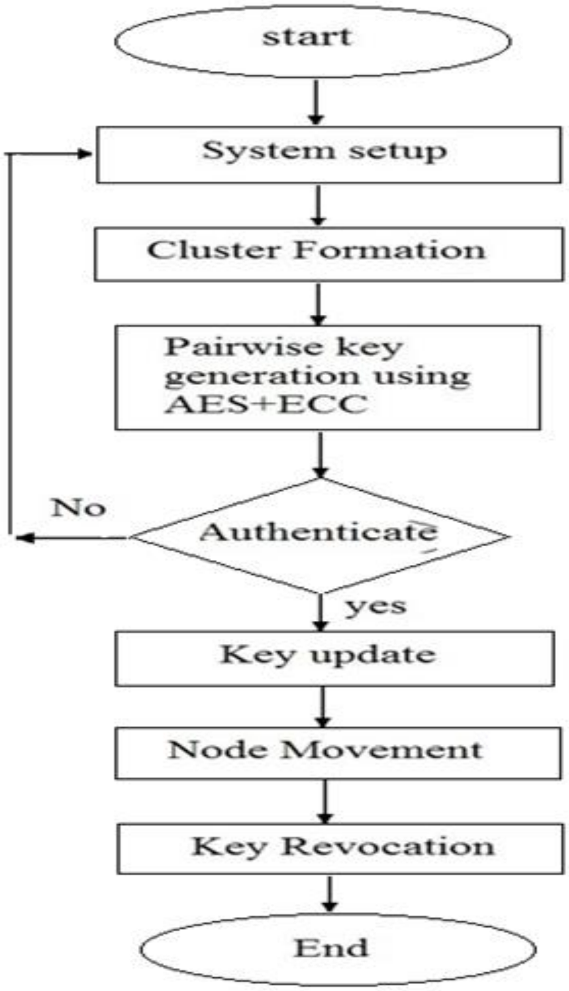
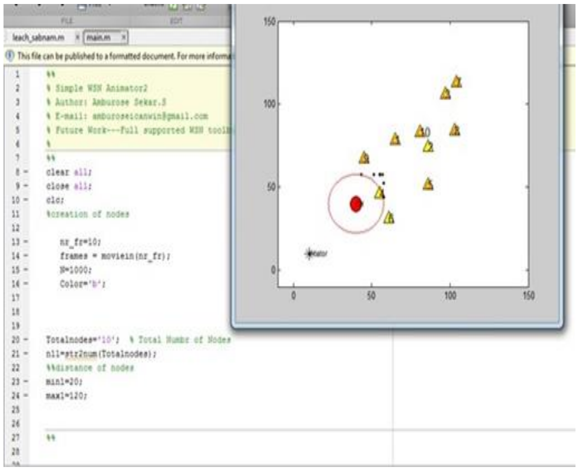


Fig.4 Flow chart of Proposed Work

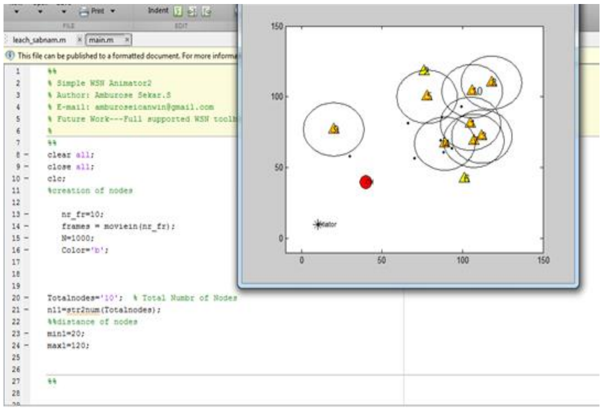
V.IMPLEMENTATION RESULT

Cluster head to Node communication


FILE
EDIT
leach_sabnam.m
main.m
This file can be published to a formatted document. For more informa
150
100
50
0
0
50
100
150

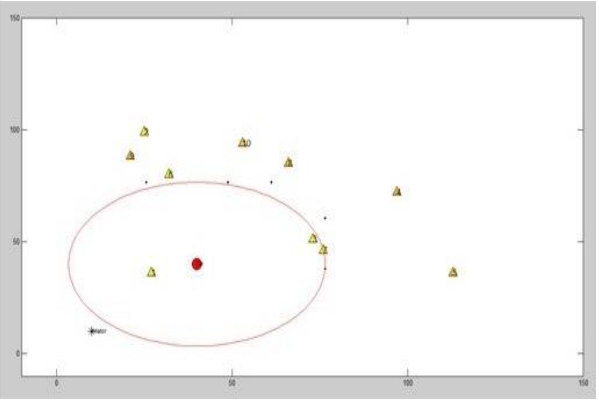
```
%%
% Simple WSN Animator2
% Author: Amburose Sekar.S
% E-mail: amburoseicanwin@gmail.com
% Future Work---Full supported WSN toolb
%
%%
clear all;
close all;
clc;
%creation of nodes

    nr_fr=10;
    frames = moviein(nr_fr);
    N=1000;
    Color='b';



Totalnodes='10';  % Total Numbr of Nodes
n11=str2num(Totalnodes);
%%distance of nodes
min1=20;
max1=120;


%%
```

Node to Cluster Head communication

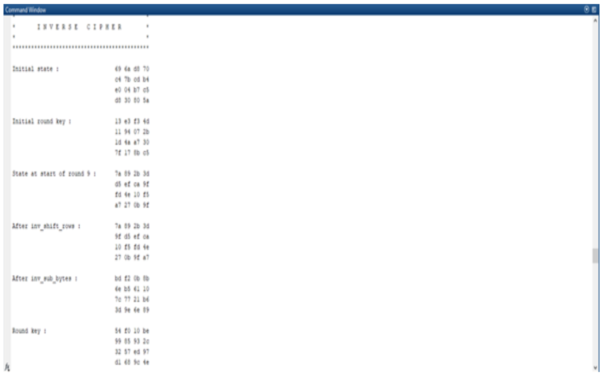

Print
Indent
FILE
EDIT
leach_sabnam.m
main.m
This file can be published to a formatted document. For more informa
150
100
50
0
0
50
100
150

```
%%
% Simple WSN Animator2
% Author: Amburose Sekar.S
% E-mail: amburoseicanwin@gmail.com
% Future Work---Full supported WSN toolb
%
%%
clear all;
close all;
clc;
%creation of nodes

    nr_fr=10;
    frames = moviein(nr_fr);
    N=1000;
    Color='b';



Totalnodes='10';  % Total Numbr of Nodes
n11=str2num(Totalnodes);
%%distance of nodes
min1=20;
max1=120;


%%
```

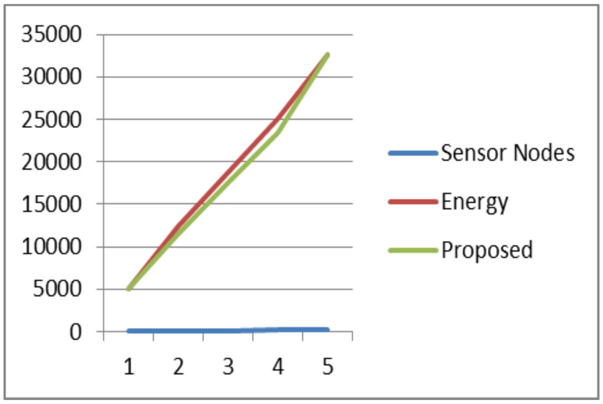
Simulation process



Key generation process



```
*      I N V E R S E   C I P H E R      *
*                                       *
*****************************************


Initial state :                   49 4a d8 70
                                  c4 7b cd b4
                                  e0 04 b7 c5
                                  d8 30 80 5a


Initial round key :               13 e3 f3 4d
                                  11 94 07 2b
                                  1d 4a a7 30
                                  7f 17 8b c5


State at start of round 9 :       7a 89 2b 3d
                                  d5 ef ca 9f
                                  fd 4e 10 f5
                                  a7 27 0b 9f


After inv_shift_rows :            7a 89 2b 3d
                                  9f d5 ef ca
                                  10 f5 fd 4e
                                  27 0b 9f a7


After inv_sub_bytes :             bd f2 0b 8b
                                  4e b5 41 10
                                  7c 77 21 b6
                                  3d 9e 4e 89


Round key :                       54 f0 10 be
                                  99 85 93 2c
                                  32 57 ed 97
                                  d1 68 9c 4e
```



VI. CONCLUSION & FUTURE WORK

As we have reviewed so many challenges in WSN Security by referring various research work, we founded Certification Less Effective Key Management scheme has better solution for secure and effective routing provision. Current work is using AES key for CL-EKM based scheme, we have founded that ECC can be applied and we can generate the Hybrid Model to generate the more secure keys. We applied the same Scheme for CL-EKM Scheme.

In Future, We will compare the result of our proposed system with various other schemes in parameter including Energy Consumptions and Security.

REFERENCES

[1] Dieynaba Mall1, Karim Konaté1, and Al-Sakib Khan Pathan , "ECL-EKM: An Enhanced Certificateless Effective Key Management Protocol for Dynamic WSN " 2017/IEEE.

[2] I.-H. Chuang, W.-T.Su, C.-Y.Wu, J.-P.Hsu, and Y.-H. Kuo, "Two layered dynamic keymanagement in mobile and long-livedclusterbased wireless sensor networks,"in Proc. IEEE WCNC, Mar. 2007, pp. 4145– 4150.

[3] M. Rahman and K. El-Khatib, in "Private key agreement and secure communication for heterogeneous sensor networks," J. Parallel Distrib.Comput., vol. 70, no. 8, pp. 858–870, 2010.

[4] Khawla Naji Shnaikat1 and Ayman Ahmed Alqudah,"Key Management Techniqes in Wireless Sensor Networks" ,2014/IJNSA.

[5] Arpandeep Kaur, Harwinder Singh Sohal, Ajay Shiv Sharma, Kuljit Kaur , "A Rigid Relationship BasedKey Security (RRBKS) Algorithm for WSN's", 2015/IEEE.

[6] Biji Niar, C. Mala , "Analysis of ECC for Application Specific WSN Security," 2015/IEEE

[7] Gagandeep Kaur, Deepali,and Rekha Kalra,"Improvement and Analyse Security of WSN From Passive Attack", 2016/IEEE.

[8] Aditi Rani, Sanjeet Kumar, "A Survey of security in Wireless Sensor Networks,"2017/IEEE.

[9] Mr. Sanket Patil1, Prof. Mrs. Snehal Bhosale , "An Improve CL-EKM Based Key management system,"2017/IJARCCE.

[10] Madhumita Panda in "Data Security in Wireless Sensor Networks via AES Algorithm" on IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015.